ФАКУЛЬТЕТ СОЦІОЛОГІЇ ТА УПРАВЛІННЯ
ЗАПОРІЗЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ

ЗАТВЕРДЖУЮ

Декан факультету соціології та управління

_____ Т.Ф. Бірюкова

«_____»_____2024 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КІБЕРБЕЗПЕКА ТА НАЦІОНАЛЬНА ПОЛІТИКА

підготовки бакалаврів

денної форми здобуття освіти

освітньо-професійна програма Політологія

спеціальності 052 Політологія

галузі знань 05 Соціальні та поведінкові науки

ВИКЛАДАЧ: Цокур Євген Георгійович, д.політ.н., доц., в.о. зав. кафедри політології

Обговорено та ухвалено
на засіданні кафедри політології

Протокол №_____від "___"_____2024 р.
Завідувач кафедри політології_____

_____
(підпис) (ініціали, прізвище)

Погоджено
Гарант освітньо-професійної програми

_____
(підпис) (ініціали, прізвище)

2024 рік

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Силабус навчальної дисципліни

Зв`язок з викладачем:
E-mail: thcokur2004@ukr.net
Телефон: 067 612 94 20
Інші засоби зв'язку: Moodle (форум курсу, приватні повідомлення); Telegram за номером 067 612 94 20
Кафедра: політології, 4 корп. ЗНУ, вул. Дніпровська, 33а

1. Опис навчальної дисципліни

Мета вивчення навчальної дисципліни «Кібербезпека та національна політика» сформувати у студентів цілісне уявлення про роль сучасних інформаційних технологій у державно-політичних процесах, їхній вплив на формування і підтримання системи національної безпеки, можливості використання таких технологій у політичній боротьбі, протистоянні держав, а також осмислити систему політичних феноменів, що визначають формування кібербезпеки.

Курс є необхідною складовою вивчення комплексу професійно-орієнтованих дисциплін, що включені до програми підготовки бакалаврів із зазначеної спеціальності. Вивчення дисципліни є важливим з огляду на її значення для формування уявлення майбутніх політологів про можливості безпечного використання сучасних інформаційних технологій у функціонуванні політичних організацій та державних установ.

У концептуальному, інформаційному і логічному плані даний курс тісно пов'язаний з такими дисциплінами, як «Політичні комунікації», «Політичні технології», «Політичний менеджмент».

Паспорт навчальної дисципліни

Нормативні показники	денна форма здобуття освіти	заочна форма здобуття освіти
Статус дисципліни	**Вибіркова**	
Семестр	7-й	
Кількість кредитів ECTS	9	
Кількість годин	270	
Лекційні заняття	30 год.	
Семінарські заняття	20 год.	
Практичні заняття		
Лабораторні заняття		
Самостійна робота	220 год.	
Консультації	Розклад розміщення консультацій: https://sites.znu.edu.ua/cms/index.php?action=news/view_details&news_id=37023&lang=ukr&news_code=tsokur---vgen-georgijovich Кількість: 2 год. особисті – субота, з 9:00 до 11:30, IV корпус, ауд. 313; дистанційні – Zoom, за попередньою домовленістю Запис на консультації: thcokur2004@ukr.net	
Вид підсумкового семестрового контролю:	**екзамен**	
Посилання на електронний курс у СЕЗН ЗНУ (платформа Moodle)	https://moodle.znu.edu.ua/course/view.php?id=12611	

2. Методи досягнення запланованих освітньою програмою компетентностей і результатів навчання

Результати навчання та компетентності	Методи навчання / форми і методи оцінювання
СК03. Здатність описувати, пояснювати й оцінювати політичні процеси та явища у різних історичних, соціальних, культурних та ідеологічних контекстах. РН05. Вміти використовувати інформаційні та комунікаційні технології у професійній діяльності.	Опрацювання першоджерел; опитування на практичних заняттях; тестування в системі Moodle; написання есе; завдання на порівняльний аналіз
СК04. Здатність застосовувати інструментарій нормативної та емпіричної політичної теорії, політичної методології, порівняльної та прикладної політології, міжнародних та глобальних студій у фаховій діяльності. РН13.Використовувати методи аналізу та оцінювання програм сталого розвитку РН11. Застосовувати інструментарій нормативної та емпіричної політичної теорії, політичної методології, порівняльної та прикладної політології, міжнародних та глобальних студій у фаховій діяльності.	Відповіді на практичних заняттях Підготовка індивідуального дослідницького завдання аналітичного характеру.
СК07. Здатність застосовувати теорії та методи прикладної політології, політичних комунікацій, спеціальних політологічних дисциплін у професійній діяльності РН15. Конструювати дизайн, розробляти програму та виконувати політологічні дослідження з використанням сучасних методів, технологій та інструментарію політичного аналізу.	Написання та усний захист індивідуального дослідницького завдання аналітичного характеру з презентацією його результатів

3. Зміст навчальної дисципліни

Змістовий модуль 1. Теоретичні аспекти кібербезпеки

Основи інформаційної та кібернетичної діяльності.

Природа інформації. Роль і місце інформації у життєдіяльності людини, суспільства. Засоби передачі та сприйняття інформації. Поняття «дані», «відомості», «інформація». Співвідношення «право держави» та «право людини» на інформацію. Властивості інформації. Вплив інформації на свідомість та поведінку людини.

Кіберсоціалізація.

Інформаційна безпека в умовах кіберцивілізації. Витоки та сутність кіберсоціалізації Соціальні мережі. Мережна мобілізація (мобілізація користувачів Інтернету через соціальні мережі). Наслідки кіберсоціалізації. Сутність поняття «кіберцивілізація». Потенційні загрози кіберцивілізації для людства. Основні риси інформаційного суспільства. Передумови успішності розвитку інформаційного суспільства в Україні.

Змістовий модуль 2. Кібербезпека в Україні і світі

Безпека інформаційної діяльності.

Інформаційна безпека. Кібербезпека. Визначення поняття «інформаційна безпека». Визначення об'єктів інформаційної небезпеки. Ієрархія об'єктів інформаційної небезпеки. Основні положення і доктрини інформаційної безпеки України. Брехня, обман та дезінформація як головні чинники маніпуляції. Маніпулювання свідомістю за допомогою засобів масової інформації. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки. Соціальні мережі: особливості, основні поняття та визначення. Моніторинг соціальних мереж — цілі та способи реалізації. Поняття соціотехнічної системи та її властивостей. Забезпечення інформаційної безпеки в мережі Інтернет.

Забезпечення кібербезпеки України в контексті проблеми національної безпеки.

Загальна характеристика законодавчих актів в сфері захисту інформації. Захист інформації як об'єкт адміністративно-правового регулювання. Система органів регулювання технічного захисту інформації України. Взаємодія суб'єктів системи технічного захисту інформації. Етапи життєвого циклу засобів захисту інформації та їх характеристика. Питання сертифікації продукції в сфері захисту інформації. Державна експертиза у сфері захисту інформації.

Змістовий модуль 3. Технологічні аспекти забезпечення кібербезпеки інформаційних систем.

Сутність та класифікація кібератак на інформаційні системи.

Класифікація автоматизованих систем в НД ТЗІ. Моделі захисту інформації в автоматизованій системі. Модель порушника інформаційної безпеки. Порядок і правила захисту інформації в КС/АС. Забезпечення доступності й цілісності інформації в АС. Провідні світові та національні органи зі стандартизації. Нормативне регулювання у сфері інформаційної безпеки в ЄС. Підходи країн ЄС та НАТО щодо регулювання питань кібернетичної безпеки.

Характеристика сучасних кібератак на інформаційно-комунікаційні системи.

Дослідження інцидентів. Надання допомоги та рекомендацій з питань протидії кіберзагрозам. Моніторинг і виявлення інцидентів. Накопичення та проведення аналізу даних про кіберзагрози. Система виявлення атак (вторгнень) (Intrusion Detection System, IDS). Виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними. Система запобігання вторгненням (Intrusion Prevention System, IPS). IPS як розширення систем виявлення вторгнень (IDS).

Змістовий модуль 4. Практичні аспекти забезпечення кібербезпеки

Етика роботи у кібербезпеці.

Поняття, принципи комп'ютерної етики. Кодекс комп'ютерної етики. Хакерська етика. Філософія штучного інтелекту. Етичні проблеми створення штучного розуму. Комп'ютерна етика як професійна. Етика інформаційної та кібербезпеки. Методи та механізми розв'язання основних моральних дилем сучасних практик в сфері управління

Організаційний рівень безпеки та підготовки фахівців з кібербезпеки.

Американський досвід підготовки фахівців із кібербезпеки на базі навчальних закладів США. Особливості стандартизації підготовки фахівців у сфері кібербезпеки в Україні. Підготовка висококваліфікованих кадрів з кібербезпеки для органів публічної влади як ключовий елемент ефективного політико-державного управління.

4. Теми лекційних занять

№ змістового модуля	Назва теми	Кількість годин		Згідно з розкладом
		о/д.ф.	з.ф.	
1	Тема 1. Основи інформаційної та кібернетичної діяльності.	4		*щотижня*
	Тема 2 Кіберсоціалізація.	3		*щотижня*
2	Тема 3. Безпека інформаційної діяльності	4		*щотижня*
	Тема 4. Забезпечення кібербезпеки України в контексті проблеми національної безпеки.	4		*щотижня*
3	Тема 5. Сутність та класифікація кібератак на інформаційні системи.	4		*щотижня*
	Тема 6. Характеристика сучасних кібератак на інформаційно-комунікаційні системи.	3		*щотижня*
4	Тема 7. Етика роботи у кібербезпеці.	4		*щотижня*
	Тема 8. Організаційний рівень безпеки та підготовки фахівців з кібербезпеки.	4		*щотижня*
Разом		30		

6. Теми семінарських занять

№ змістового модуля	Назва теми	Кількість годин		Згідно з розкладом
		о/д.ф.	з.ф.	
1	Основи інформаційної та кібернетичної діяльності. План. 1.Природа інформації. 2.Роль і місце інформації у життєдіяльності людини, суспільства. 3.Засоби передачі та сприйняття інформації. 4.Поняття «дані», «відомості», «інформація».	3		*щотижня*
	Кіберсоціалізація. План. 1.Інформаційна безпека в умовах кіберцивілізації. 2.Витоки та сутність кіберсоціалізації. 3. Соціальні мережі.	2		*щотижня*
2	Безпека інформаційної діяльності. План. 1.Інформаційна безпека. 2.Кібербезпека. 3.Визначення поняття «інформаційна безпека». 4.Визначення об’єктів інформаційної небезпеки. 5. Брехня, обман та дезінформація як головні чинники маніпуляції.	3		*щотижня*

	Забезпечення кібербезпеки України в контексті проблеми національної безпеки. План. 1.Загальна характеристика законодавчих актів в сфері захисту інформації. 2. Захист інформації як об'єкт адміністративно-правового регулювання. 3. Система органів регулювання технічного захисту інформації України.	2		*щотижня*
3	Сутність та класифікація кібератак на інформаційні системи. План. 1.Класифікація автоматизованих систем в НД ТЗІ. 2.Моделі захисту інформації в автоматизованій системі. 3.Модель порушника інформаційної безпеки. 4. Порядок і правила захисту інформації в КС/АС. 5.Забезпечення доступності й цілісності інформації в АС.	3		*щотижня*
	Характеристика сучасних кібератак на інформаційно-комунікаційні системи. План. 1.Дослідження інцидентів. 2.Надання допомоги та рекомендацій з питань протидії кіберзагрозам. 3.Моніторинг і виявлення інцидентів. 4.Накопичення та проведення аналізу даних про кіберзагрози. 5.Система виявлення атак (вторгнень) (Intrusion Detection System, IDS).	2		*щотижня*
4	Етика роботи у кібербезпеці. План. 1.Поняття, принципи комп'ютерної етики. 2.Кодекс комп'ютерної етики. 3.Хакерська етика. Філософія штучного інтелекту. 4.Етичні проблеми створення штучного розуму. 5.Комп'ютерна етика як професійна.	3		*щотижня*
	Організаційний рівень безпеки та підготовки фахівців з кібербезпеки. План. 1.Американський досвід підготовки фахівців із кібербезпеки на базі навчальних закладів США. 2.Особливості стандартизації підготовки фахівців у сфері кібербезпеки в Україні.	2		*щотижня*
Разом		20		

3. Самостійна робота

№ змістового модуля	Питання для самостійного опрацювання	Кількість годин	
		о/д.ф.	з.ф.
1	1.Співвідношення «право держави» та «право людини» на інформацію. 2.Властивості інформації. 3.Вплив інформації на свідомість та поведінку людини. 4.Мережна мобілізація (мобілізація користувачів Інтернету через соціальні мережі). 5.Наслідки кіберсоціалізації. 6.Сутність поняття «кіберцивілізація». 7. Потенційні загрози кіберцивілізації для людства. 8. Основні риси інформаційного суспільства. 9.Передумови успішності розвитку інформаційного суспільства в Україні.	55	
2	1.Маніпулювання свідомістю за допомогою засобів масової інформації. 2. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. 3.Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки. 4.Соціальні мережі: особливості, основні поняття та визначення. 5.Моніторинг соціальних мереж – цілі та способи реалізації. 6.Поняття соціотехнічної системи та її властивостей. 7.Забезпечення інформаційної безпеки в мережі Інтернет. 8. Взаємодія суб'єктів системи технічного захисту інформації. 9. Етапи життєвого циклу засобів захисту інформації та їх характеристика. 10. Питання сертифікації продукції в сфері захисту інформації. 11.Державна експертиза у сфері захисту інформації.	55	
3	1.Провідні світові та національні органи зі стандартизації. 2.Нормативне регулювання у сфері інформаційної безпеки в ЄС. 3.Підходи країн ЄС та НАТО щодо регулювання питань кібернетичної безпеки. 4.Виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними. 5.Система запобігання вторгненням (Intrusion Prevention System, IPS). IPS як розширення систем виявлення вторгнень (IDS).	55	
4	1.Етика інформаційної та кібербезпеки. 2. Методи та механізми розв'язання основних моральних дилем сучасних практик в сфері управління 3.Підготовка висококваліфікованих кадрів з кібербезпеки для органів публічної влади як ключовий елемент ефективного політико-державного управління.	55	
Разом		220	

4. Види і зміст поточних контрольних заходів

№ змістового модуля	Вид поточного контрольного заходу	Зміст поточного контрольного заходу*	Критерії оцінювання та термін виконання	Усього балів
1	Опитування, тести	Практичне заняття 1 Питання для підготовки до практичного заняття 1.Природа інформації. 2.Роль і місце інформації у життєдіяльності людини, суспільства. 3.Засоби передачі та сприйняття інформації. 4.Поняття «дані», «відомості», «інформація». Посилання на тест: https://moodle.znu.edu.ua/course/view.php?id=12611	3 бали – глибокі і систематичні знання теорії, здатність вирішувати проблемні питання. Відповідь відрізняється точністю формулювань, логікою, достатній рівень узагальненості знань. Наявна авторська позиція 2 бали – студент знає і може самостійно сформулювати основні поняття теми та пов'язати їх з реальними явищами. Відповідь логічна, але змістовно неповна. 1 бал – студент відтворює основні поняття і визначення, але досить поверхово, не виділяючи взаємозв'язок між ними, може сформулювати з допомогою викладача основні положення теми. Відповідь фрагментарна Тест: мах 2 бали	5
	Опитування, тести	Практичне заняття 2 Питання для підготовки до практичного заняття 1.Інформаційна безпека в умовах кіберцивілізації. 2.Витоки та сутність кіберсоціалізації. 3. Соціальні мережі. Посилання на тест: https://moodle.znu.edu.ua/course/view.php?id=12611	3 бали – глибокі і систематичні знання теорії, здатність вирішувати проблемні питання. Відповідь відрізняється точністю формулювань, логікою, достатній рівень узагальненості знань. Наявна авторська позиція 2 бали – студент знає і може самостійно сформулювати основні поняття теми та пов'язати їх з реальними явищами. Відповідь логічна, але змістовно неповна. 1 бал – студент відтворює основні поняття і визначення, але досить поверхово, не виділяючи взаємозв'язок між ними, може сформулювати з допомогою викладача основні положення теми. Відповідь фрагментарна Тест: мах 2 бали	5
	Тести, есе	Контрольна робота: Виконання тесту https://moodle.znu.edu.ua/course/view.php?id=12611 написання есе за 1 змістовим модулем	Тест: мах 2 бали Есе: Розгорнутий роздум з власною позицією –3 бали Розгорнута відповідь, але без власної позиції – 2 бали Виклад змісту есе не відповідає вимогам до структури – 1бал Виконується наприкінці поточного модулю.	5
2	Опитування, тести	Практичне заняття 3 Питання для підготовки до практичного заняття 1.Інформаційна безпека. 2.Кібербезпека. 3.Визначення поняття «інформаційна безпека».	3 бали – глибокі і систематичні знання теорії, здатність вирішувати проблемні питання. Відповідь відрізняється точністю формулювань, логікою, достатній рівень узагальненості знань. Наявна авторська позиція	5

		4.Визначення об’єктів інформаційної небезпеки. 5. Брехня, обман та дезінформація як головні чинники маніпуляції. Посилання на тест: https://moodle.znu.edu.ua/course/view.php?id=12611	2 бали – студент знає і може самостійно сформулювати основні поняття теми та пов'язати їх з реальними явищами. Відповідь логічна, але змістовно неповна. 1 бал – студент відтворює основні поняття і визначення, але досить поверхово, не виділяючи взаємозв'язок між ними, може сформулювати з допомогою викладача основні положення теми. Відповідь фрагментарна Тест: мах 2 бали	
	Опитування, тести	Практичне заняття 4 Питання для підготовки до практичного заняття 1.Загальна характеристика законодавчих актів в сфері захисту інформації. 2. Захист інформації як об’єкт адміністративно-правового регулювання. 3. Система органів регулювання технічного захисту інформації України. Посилання на тест: https://moodle.znu.edu.ua/course/view.php?id=12611	3 бали – глибокі і систематичні знання теорії, здатність вирішувати проблемні питання. Відповідь відрізняється точністю формулювань, логікою, достатній рівень узагальненості знань. Наявна авторська позиція 2 бали – студент знає і може самостійно сформулювати основні поняття теми та пов'язати їх з реальними явищами. Відповідь логічна, але змістовно неповна. 1 бал – студент відтворює основні поняття і визначення, але досить поверхово, не виділяючи взаємозв'язок між ними, може сформулювати з допомогою викладача основні положення теми. Відповідь фрагментарна Тест: мах 2 бали	5
2	Тести, есе	Контрольна робота Виконання тесту https://moodle.znu.edu.ua/course/view.php?id=12611 написання есе за 2 змістовим модулем	Тест: мах 2 бали Есе: Розгорнутий роздум з власною позицією – 3 бали Розгорнута відповідь, але без власної позиції – 2 бали Виклад змісту есе не відповідає вимогам до структури – 1бал Виконується наприкінці поточного модулю.	5
3	Опитування, тести	Практичне заняття 5 Питання для підготовки до практичного заняття 1.Класифікація автоматизованих систем в НД ТЗІ. 2.Моделі захисту інформації в автоматизованій системі. 3.Модель порушника інформаційної безпеки. 4. Порядок і правила захисту інформації в КС/АС. 5.Забезпечення доступності й цілісності інформації в АС. Посилання на тест: https://moodle.znu.edu.ua/course/view.php?id=12611	3 бали – глибокі і систематичні знання теорії, здатність вирішувати проблемні питання. Відповідь відрізняється точністю формулювань, логікою, достатній рівень узагальненості знань. Наявна авторська позиція 2 бали – студент знає і може самостійно сформулювати основні поняття теми та пов'язати їх з реальними явищами. Відповідь логічна, але змістовно неповна. 1 бал – студент відтворює основні поняття і визначення, але досить поверхово, не виділяючи взаємозв'язок між ними, може сформулювати з допомогою викладача основні положення теми. Відповідь фрагментарна Тест: мах 2 бали	5
		Практичне заняття 6 Питання для підготовки до практичного заняття 1.Дослідження інцидентів. 2.Надання допомоги та рекомендацій з питань протидії	3 бали – глибокі і систематичні знання теорії, здатність вирішувати проблемні питання. Відповідь відрізняється точністю формулювань, логікою, достатній рівень узагальненості знань. Наявна	5

		кіберзагрозам. 3.Моніторинг і виявлення інцидентів. 4.Накопичення та проведення аналізу даних про кіберзагрози. 5.Система виявлення атак (вторгнень) (Intrusion Detection System, IDS). Посилання на тест: https://moodle.znu.edu.ua/course/view.php?id=12611	авторська позиція 2 бали – студент знає і може самостійно сформулювати основні поняття теми та пов'язати їх з реальними явищами. Відповідь логічна, але змістовно неповна. 1 бал – студент відтворює основні поняття і визначення, але досить поверхово, не виділяючи взаємозв'язок між ними, може сформулювати з допомогою викладача основні положення теми. Відповідь фрагментарна Тест: мах 2 бали	
3	Тести, есе	Контрольна робота Виконання тесту https://moodle.znu.edu.ua/course/view.php?id=12611 написання есе за 3 змістовим модулем	Тест: мах 2 бали Есе: Розгорнутий роздум з власною позицією – 3 бали Розгорнута відповідь, але без власної позиції –2 бали Виклад змісту есе не відповідає вимогам до структури – 1бал Виконується наприкінці поточного модулю	5
4	Опитування, тести	Практичне заняття 7 Питання для підготовки до практичного заняття 1.Поняття, принципи комп'ютерної етики. 2.Кодекс комп'ютерної етики. 3.Хакерська етика. Філософія штучного інтелекту. 4.Етичні проблеми створення штучного розуму. 5.Комп'ютерна етика як професійна. Посилання на тест: https://moodle.znu.edu.ua/course/view.php?id=12611	3 бали – глибокі і систематичні знання теорії, здатність вирішувати проблемні питання. Відповідь відрізняється точністю формулювань, логікою, достатній рівень узагальненості знань. Наявна авторська позиція 2 бали – студент знає і може самостійно сформулювати основні поняття теми та пов'язати їх з реальними явищами. Відповідь логічна, але змістовно неповна. 1 бал – студент відтворює основні поняття і визначення, але досить поверхово, не виділяючи взаємозв'язок між ними, може сформулювати з допомогою викладача основні положення теми. Відповідь фрагментарна Тест: мах 2 бали	5
	Опитування, тести	Практичне заняття 8 Питання для підготовки до практичного заняття 1.Американський досвід підготовки фахівців із кібербезпеки на базі навчальних закладів США. 2.Особливості стандартизації підготовки фахівців у сфері кібербезпеки в Україні. Посилання на тест: https://moodle.znu.edu.ua/course/view.php?id=12611	3 бали – глибокі і систематичні знання теорії, здатність вирішувати проблемні питання. Відповідь відрізняється точністю формулювань, логікою, достатній рівень узагальненості знань. Наявна авторська позиція 2 бали – студент знає і може самостійно сформулювати основні поняття теми та пов'язати їх з реальними явищами. Відповідь логічна, але змістовно неповна. 1 бал – студент відтворює основні поняття і визначення, але досить поверхово, не виділяючи взаємозв'язок між ними, може сформулювати з допомогою викладача основні положення теми. Відповідь фрагментарна Тест: мах 2 бали	5
4	Тести, есе	Контрольна робота Виконання тесту https://moodle.znu.edu.ua/course/view.php?id=12611 написання есе за 4 змістовим модулем	Тест: мах 2 бали Есе: Розгорнутий роздум з власною позицією – 3 бали Розгорнута відповідь, але без власної позиції –2 бали	5

			Виклад змісту есе не відповідає вимогам до структури – 1бал Виконується наприкінці поточного модулю	
Усього за змістові модулі	**11**			**60**

5. Підсумковий семестровий контроль

Форма	Види підсумкових контрольних заходів	Зміст підсумкового контрольного заходу	Критерії оцінювання	Усього балів
1	**2**	**3**	**4**	**5**
екзамен	Теоретичне завдання	Питання для підготовки: 1.Природа інформації. 2.Роль і місце інформації у життєдіяльності людини, суспільства. 3.Засоби передачі та сприйняття інформації. 4.Поняття «дані», «відомості», «інформація». 5.Інформаційна безпека в умовах кіберцивілізації. 6.Витоки та сутність кіберсоціалізації. 7. Соціальні мережі. 8.Інформаційна безпека. 9.Кібербезпека. 10.Визначення поняття «інформаційна безпека». 11.Визначення об'єктів інформаційної небезпеки. 12. Брехня, обман та дезінформація як головні чинники маніпуляції. 13.Загальна характеристика законодавчих актів в сфері захисту інформації. 14.Захист інформації як об'єкт адміністративно-правового регулювання. 15.Система органів регулювання технічного захисту інформації України. 16.Класифікація автоматизованих систем в НД ТЗІ. 17.Моделі захисту інформації в автоматизованій системі. 18.Модель порушника інформаційної безпеки. 19. Порядок і правила захисту інформації в КС/АС. 20.Забезпечення доступності й цілісності інформації в АС. 21.Дослідження інцидентів. 22.Надання допомоги та рекомендацій з питань протидії кіберзагрозам. 23.Моніторинг і виявлення інцидентів. 24.Накопичення та проведення аналізу даних про кіберзагрози. 25.Система виявлення атак (вторгнень) (Intrusion Detection System, IDS). 26.Поняття, принципи комп'ютерної етики. 27.Кодекс комп'ютерної етики. 28.Хакерська етика. 29.Філософія штучного інтелекту. 30.Етичні проблеми створення штучного розуму. 31.Комп'ютерна етика як професійна. 32.Американський досвід підготовки	2 питання, відповідь на кожне оцінюється у 10 балів 10-9 балів – глибокі і систематичні знання теорії, здатність вирішувати проблемні питання. Відповідь відрізняється точністю формулювань, логікою, достатній рівень узагальненості знань. Наявна авторська позиція 8-7 бали – глибокі і систематичні знання теорії, здатність вирішувати проблемні питання. Відповідь студента відрізняється точністю формулювань, логікою, достатній рівень узагальненості знань. 6-5 балів – студент знає і може самостійно сформулювати основні поняття теми та пов'язати їх з реальними явищами. Проте відповідь змістовно неповна. Відповідь логічна, але розуміння не є узагальненим 4-3 бали – студент відтворює основні поняття і визначення, але досить поверхово, не виділяючи взаємозв'язок між ними, може сформулювати з допомогою викладача основні положення теми, допускає помилки, які повною мірою самостійно виправити не може 2-1 бал - відповідь студента фрагментарна, зумовлена нечіткими уявленнями про закони і явища. У відповіді цілком відсутня самостійність	**20**

		фахівців із кібербезпеки на базі навчальних закладів США. 33.Особливості стандартизації підготовки фахівців у сфері кібербезпеки в Україні.		
		Тести - 10 питань, розміщені у Moodle.	1 бал за кожну правильну відповідь. На проходження тесту дається 15 хвилин і одна спроба	**10**
	Практичне завдання	написання екзаменаційного есе. **Есе** складається з таких структурних елементів: - вступ, де студент формулює власну точку зору на проблему, винесену як тему есе; - блок аргументації: три і більше аргументи, що підтверджують точку зору автора; - висновки, де відбувається узагальнення авторської позиції і відбувається підтвердження вихідної тези на більш високому доказовому рівні. Оскільки головна мета есе – змусити читача розділити точку зору автора, важливо використовувати риторичні фігури переконання, маркери логічної послідовності елементів («по-перше», «по-друге», «з вищезазначеного витікає» та ін.), апелювати до спільних соціальних та духовних цінностей, поглядів, знань та фактів (дослідження, статистичні дані, думки фахівців, приклади з життя), проводити ефектні паралелі й аналогії для демонстрації вашої ерудиції, вдало використовувати цитати з прочитаної наукової літератури.	10-9 – робота повністю розкриває тему, логічно структурована, оперування багатьма теоретичними поняттями, висока аргументованість відповіді, наведення прикладів з політичної практики 8-7 – положення та висновки недостатньо аргументовані, але робота достатньо логічна 6-5 – недостатньо чітка структура, аргументація положень має незавершений характер, розмита конкретика 4-3 – відсутня чітка структура, описовий характер 2-1 – робота фрагментарна, відсутня логіка та структура	**10**
Усього за підсумковий семестровий контроль				**40**

Шкала оцінювання ЗНУ: національна та ECTS

За шкалою ECTS	За шкалою університету	За національною шкалою	
		Екзамен	Залік
A	90 – 100 (відмінно)	5 (відмінно)	Зараховано
B	85 – 89 (дуже добре)	4 (добре)	
C	75 – 84 (добре)		
D	70 – 74 (задовільно)	3 (задовільно)	
E	60 – 69 (достатньо)		
FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)	Не зараховано
F	1 – 34 (незадовільно – з обов'язковим повторним курсом)		

9. Рекомендована література

Основна:

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ : ДУТ, 2015. 288 с.
2. Бурячок В. Л. Інформаційний та кіберпростори : проблеми безпеки, методи та засоби боротьби. Навчальний посібник. Київ : ДУТКНУ, 2016. 178 с.
3. Вишня В. Б. , Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посібник. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
4. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. Київ : Видавництво НА СБ України, 2015. 251 с.
5. Кавун С. В. Інформаційна безпека : навч. посіб. Харків : ХНЕУ, 2008. 352с.

Додаткова:

1. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. Київ : ДУІКТ, 2010. 454 с.
2. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. Киїав :ДУТ, 2015. 345 с.
3. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. Монографія. Київ : ДУТ, 2015. 124 С.
4.Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник. Київ: ВІКНУ, 2016. 286 с.
5.Jajodia S., Shakarian P., Subrahmanian V.S., Swarup V. Cyber Warfare: Building the Scientific Foundation. London: Springer, 2015. 321 p. 6. Binary bullets: the ethics of cyberwarfare / edited by F.Allhoff, A.Henschke, B.J.Strawser. New York: Oxford University Press, 2016. 296 p.
6.Greenberg A. Sandworm : a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. New York : Doubleday, 2019. 370 p.

10. Інформаційні ресурси

1. Державна служба спеціального зв'язку та захисту інформації. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/index.

2Концепція інформаційної безпеки України. URL :https://www.osce.org/files/f/documents/0/2/175056.pdf

3. Морозова Т. Ю. Про необхідність вивчення комп'ютерної етики майбутніми IT-фахівцями. URL: http://www.nbuv.gov.ua/portal/natural/vkpi/FPP/2006- 2/05Morozova.pdf.

4.Стратегія кібербезпеки України (2021 – 2025 роки). URL : https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt %20strategii_kyberbezpeki_Ukr.pdf

5.Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf

11. Регуляції і політики курсу

Відвідування занять. Регуляція пропусків. Інтерактивний характер курсу передбачає обов'язкове відвідування практичних занять. Студенти, які за певних обставин не можуть відвідувати практичні заняття регулярно, мусять впродовж тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущенні завдання мають бути відпрацьовані на найближчій консультації впродовж тижня після пропуску.

Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання шляхом виконання індивідуального письмового завдання. Студенти, які станом на початок екзаменаційної сесії мають понад 70% невідпрацьованих пропущених занять, до відпрацювання не допускаються.

Політика академічної доброчесності. Усі письмові роботи, що виконуються слухачами під час проходження курсу, перевіряються на наявність плагіату за допомогою спеціалізованого програмного забезпечення.

Відповідно до чинних правових норм, плагіатом вважатиметься: копіювання чужої наукової роботи чи декількох робіт та оприлюднення результату під своїм іменем; створення суміші власного та запозиченого тексту без належного цитування джерел; рерайт (перефразування чужої праці без згадування оригінального автора). Будь-яка ідея, думка чи речення, ілюстрація чи фото, яке ви запозичуєте, має супроводжуватися посиланням на першоджерело.

Виконавці індивідуальних дослідницьких завдань обов'язково додають до текстів своїх робіт власноруч підписану Декларацію академічної доброчесності (див. посилання у Додатку до силабусу). Роботи, у яких виявлено ознаки плагіату, до розгляду не приймаються і відхиляються без права перескладання. Якщо ви не впевнені, чи підпадають зроблені вами запозичення під визначення плагіату, будь ласка, проконсультуйтеся з викладачем. Висока академічна культура та європейські стандарти якості освіти, яких дотримуються у ЗНУ, вимагають від дослідників відповідального ставлення до вибору джерел. Посилання на такі ресурси, як Wikipedia, бази даних рефератів та письмових робіт (Studopedia.org та подібні) є неприпустимим. Рекомендовані бази даних для пошуку джерел: Електронні ресурси Національної бібліотеки ім. Вернадського: http://www.nbuv.gov.ua

Цифрова повнотекстова база даних англомовної наукової періодики JSTOR: https://www.jstor.org/

Використання комп'ютерів/телефонів на занятті. Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). Будь ласка, не забувайте активувати режим «без звуку» до початку заняття. Під час виконання заходів контролю (термінологічних диктантів, контрольних робіт, іспитів) використання гаджетів заборонено. У разі порушення цієї заборони роботу буде анульовано без права перескладання.

Визнання результатів неформальної/інформальної освіти

За бажанням студентів результати проходження курсів підвищення кваліфікації, стажувань, онлайн-курсів, тощо можуть бути зараховані у якості результату засвоєння відповідного змістового модулю дисципліни.

Комунікація. Базовою платформою для комунікації викладача зі студентами є Moodle. Важливі повідомлення загального характеру – зокрема, оголошення про терміни подання контрольних робіт, коди доступу до сесій у Zoom та ін. – регулярно розміщуються викладачем на форумі курсу. Для персональних запитів використовується сервіс приватних повідомлень. Відповіді на запити студентів подаються викладачем впродовж трьох робочих днів. Для оперативного отримання повідомлень про оцінки та нову інформацію, розміщену на сторінці курсу у Moodle, будь ласка, переконайтеся, що адреса електронної пошти, зазначена у вашому профайлі на Moodle, є актуальною, та регулярно перевіряйте папку «Спам». Якщо за технічних причин доступ до Moodle є неможливим, або ваше питання потребує термінового розгляду, направте електронного листа з позначкою «Важливо» на адресу ngml@ukr.net. У листі обов'язково вкажіть ваше прізвище та ім'я, курс та шифр академічної групи.

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Силабус навчальної дисципліни

ДОДАТОК ДО СИЛАБУСУ ЗНУ – 2024-2025 рр.

ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ 2024-2025 н. р. доступний за адресою: https://tinyurl.com/yckze4jd.

АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ. Студенти і викладачі Запорізького національного університету несуть персональну відповідальність за дотримання принципів академічної доброчесності, затверджених **Кодексом академічної доброчесності ЗНУ:** https://tinyurl.com/ya6yk4ad. Декларація академічної доброчесності здобувача вищої освіти (додається в обов'язковому порядку до письмових кваліфікаційних робіт, виконаних здобувачем, та засвідчується особистим підписом): https://tinyurl.com/y6wzzlu3.

НАВЧАЛЬНИЙ ПРОЦЕС ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ. Перевірка набутих студентами знань, навичок та вмінь (атестації, заліки, іспити та інші форми контролю) є невід'ємною складовою системи забезпечення якості освіти і проводиться відповідно до Положення про організацію та методику проведення поточного та підсумкового семестрового контролю навчання студентів ЗНУ: https://tinyurl.com/y9tve4lk.

ПОВТОРНЕ ВИВЧЕННЯ ДИСЦИПЛІН, ВІДРАХУВАННЯ. Наявність академічної заборгованості до 6 навчальних дисциплін (в тому числі проходження практики чи виконання курсової роботи) за результатами однієї екзаменаційної сесії є підставою для надання студенту права на повторне вивчення зазначених навчальних дисциплін. Порядок повторного вивчення визначається Положенням про порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ: https://tinyurl.com/y9pkmmp5. Підстави та процедури відрахування студентів, у тому числі за невиконання навчального плану, регламентуються Положенням про порядок переведення, відрахування та поновлення студентів у ЗНУ: https://tinyurl.com/ycds57la.

НЕФОРМАЛЬНА ОСВІТА. Порядок зарахування результатів навчання, підтверджених сертифікатами, свідоцтвами, іншими документами, здобутими поза основним місцем навчання, регулюється Положенням про порядок визнання результатів навчання, отриманих у неформальній освіті: https://tinyurl.com/y8gbt4xs.

ВИРІШЕННЯ КОНФЛІКТІВ. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, регламентуються Положенням про порядок і процедури вирішення конфліктних ситуацій у ЗНУ: https://tinyurl.com/57wha734. Конфліктні ситуації, що виникають у сфері стипендіального забезпечення здобувачів вищої освіти, вирішуються стипендіальними комісіями факультетів, коледжів та університету в межах їх повноважень, відповідно до: Положення про порядок призначення і виплати академічних стипендій у ЗНУ: https://tinyurl.com/yd6bq6p9; Положення про призначення та виплату соціальних стипендій у ЗНУ: https://tinyurl.com/y9r5dpwh.

ПСИХОЛОГІЧНА ДОПОМОГА. Телефон довіри практичного психолога **Марті Ірини Вадимівни** (061) 228-15-84, (099) 253-78-73 (щоденно з 9 до 21).

УПОВНОВАЖЕНА ОСОБА З ПИТАНЬ ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ КОРУПЦІЇ Запорізького національного університету: **Банах Віктор Аркадійович**
Електронна адреса:
v_banakh@znu.edu.uaГар
яча лінія:
(061) 227-12-76

РІВНІ МОЖЛИВОСТІ ТА ІНКЛЮЗИВНЕ ОСВІТНЄ СЕРЕДОВИЩЕ. Центральні входи усіх навчальних корпусів ЗНУ обладнані пандусами для забезпечення доступу осіб з інвалідністю та інших маломобільних груп населення. Допомога для здійснення входу у разі потреби надається черговими охоронцями навчальних корпусів. Якщо вам потрібна спеціалізована допомога, будь ласка, зателефонуйте (061) 228-75-11 (начальник охорони). Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗНУ: https://tinyurl.com/ydhcsagx.

РЕСУРСИ ДЛЯ НАВЧАННЯ.
Наукова бібліотека: http://library.znu.edu.ua. Графік роботи абонементів: понеділок-п`ятниця з 08.00 до 16.00; вихідні дні: субота і неділя.

СИСТЕМА ЕЛЕКТРОННОГО ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ (MOODLE): https://moodle.znu.edu.ua
Якщо забули пароль/логін, направте листа з темою «Забув пароль/логін» за адресою: moodle.znu@znu.edu.ua.
У листі вкажіть: прізвище, ім'я, по-батькові українською мовою; шифр групи; електронну адресу.
Якщо ви вказували електронну адресу в профілі системи Moodle ЗНУ, то використовуйте посилання для відновлення паролю https://moodle.znu.edu.ua/mod/page/view.php?id=133015.

ЦЕНТР ІНТЕНСИВНОГО ВИВЧЕННЯ ІНОЗЕМНИХ МОВ: http://sites.znu.edu.ua/child-advance/
ЦЕНТР НІМЕЦЬКОЇ МОВИ, ПАРТНЕР ГЕТЕ-ІНСТИТУТУ: https://www.znu.edu.ua/ukr/edu/ocznu/nim
ШКОЛА КОНФУЦІЯ (ВИВЧЕННЯ КИТАЙСЬКОЇ МОВИ): http://sites.znu.edu.ua/confucius